Accepted Manuscript

Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions

Sven Plaga, Norbert Wiedermann, Simon Duque Anton, Stefan Tatschner, Hans Schotten, Thomas Newe

PII: S0167-739X(18)31404-3
DOI: https://doi.org/10.1016/j.future.2018.11.008
Reference: FUTURE 4572

To appear in: *Future Generation Computer Systems*

Received date : 8 June 2018
Revised date : 8 October 2018
Accepted date : 7 November 2018

Please cite this article as: S. Plaga, N. Wiedermann, S.D. Anton et al., Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.11.008

Securing Future Decentralised Industrial IoT Infrastructures: Challenges and Free Open Source Solutions

Sven Plaga[a,c], Norbert Wiedermann[a,], Simon Duque Anton[b], Stefan Tatschner[a], Hans Schotten[b], Thomas Newe[c]

[a]*Fraunhofer Institute AISEC, Garching bei München, Germany*
Corresponding author: norbert.wiedermann@aisec.fraunhofer.de (Norbert Wiedermann)
[b]*German Research Center for Artificial Intelligence, Germany*
[c]*CONFIRM Centre for Smart Manufacturing, University of Limerick, Ireland*

Abstract

The next industrial revolution is said to be paved by the use of novel Internet of Things (IoT) technology. One important aspect of the modern IoT infrastructures is decentralised communication, often called Peer-to-Peer (P2P). In the context of industrial communication, P2P contributes to resilience and improved stability for industrial components. Current industrial facilities, however, still rely on centralised networking schemes which are considered to be mandatory to comply with security standards. In order to succeed, introduced industrial P2P technology must maintain the current level of protection and also consider possible new threats. The presented work starts with a short analysis of well-established industrial communication infrastructures and how these could benefit from decentralised structures. Subsequently, previously undefined Information Technology (IT) security requirements are derived from the new cloud based decentralised industrial automation model architecture presented in this paper. To meet those requirements, state-of-the-art communication schemes and their open source implementations are presented and assessed for their usability in the context of industrial IoT. Finally, derived building blocks for industrial IoT P2P security are presented which are qualified to comply with the stated industrial IoT security requirements.

Keywords: Industrial Internet of Things, Cyber security, Decentralisation, Smart environments, Secure communications
2010 MSC: 68M12, 68M10

1. Industrial Manufacturing

From the beginning of industrialisation, the process of manufacturing has been constantly changing. Periods of transformation are often initiated when new disruptive technologies become available to act as an enabler for emerging innovative and groundbreaking concepts. Retrospectively viewed, the history of industrialisation has experienced three such transformations. Regarding their impact on the manufacturing process these are often designated as the three industrial revolutions.

A good illustration for this is the relationship between *mechanisation* and the principle of *division of labour*. According to the findings of eighteenth-century philosopher Adam Smith, division of labour [1] is one of the driving forces in industrial manufacturing which is still present today. While the use of machines paved the way for the first industrial revolution, division of labour induced the second industrial revolution and enabled production of goods at affordable prices. Since that time, the ideology of divided labour has been continually refined and has resulted in modern supply chains.

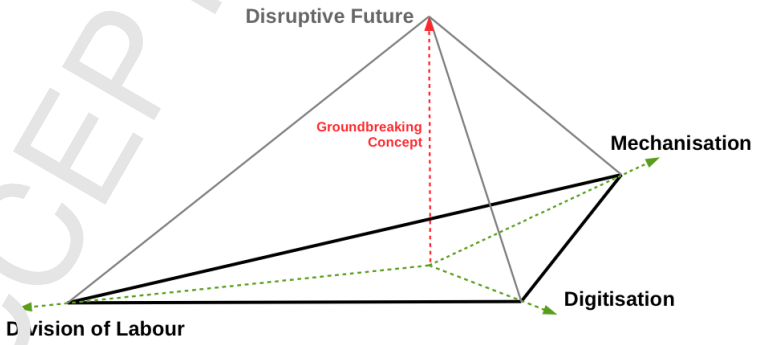

Figure 1: Forces of Industrial Manufacturing

The development of Programmable Logic Controllers (PLCs) during the mid-sixties of the twentieth century [2] introduced the capabilities of modern computer systems to the industrial production process. Among others, two positive effects of this third industrial revolution were distributed and efficient control of complex processes resulting in consistent quality.

Figure 1 illustrates the relationship of the outlined forces relevant for the current appearance and future evolution of industrial manufacturing. Because of its age, the division of labour is the most influential force, followed by mechanisation. Together with the most recently added factor, *digitisation*, these three factors form the basis for the realisation of groundbreaking concepts of the future.

An important role for future industrial manufacturing is digitisation, which has not yet reached the end of its development cycle (cp. Gartner Hype Cycle for Supply Chain Strategy [3]). In this cycle the decentralisation of previously concentrated digital resources is prominent. Among the important factors such as costs and usability, security is seen as a main challenge for this technology to succeed.

2. The Impact of Digitisation

After World War II (WW II), the theoretical foundations of computer science, initially developed for code breaking, were adapted for industrial use [4]. The invention of electronic semiconductors aided the development of integrated PLC modules. These are the baseline for modern manufacturing systems to satisfy customer demands for high quality, delivered on the basis of a short time-to-market which is critical for the success of new products.

Present industrial infrastructures are determined by two prominent characteristics. Firstly, they are organised along the well-established hierarchical industrial automation pyramid model. Traditionally, each pyramid represents a production site which is separated from other sites. Following the paradigm of division of labour, the second characteristic is the linkage of different production sites through supply chains.

2.1. Industrial Automation Pyramid

Along with the introduction of PLCs to the production proc[illegible] the classic industrial automation pyramid illustrated by figure 2 w[illegible] specifi[illegible]d.

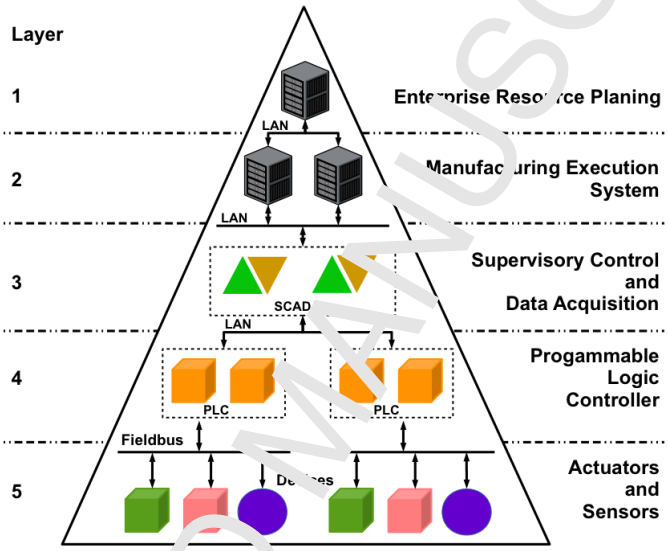

Figure 2: IEC 62264 Industrial Automation Pyramid

The automation pyramid follows a hierarchical approach where each layer has a certain purpose:

- **Enterprise Resource Planning (ERP):** This layer hosts the business-management software which is typically responsible for keeping track of raw-material flow, production capacity as well as customer orders.
- **Manufacturing Execution System (MES):** These systems are in charge of tracking and documenting the transformation of raw materials to the final products. Typically, MES are interface systems preparing data for the ERP.
- **Supervisory Control And Data Acquisition (SCADA):** This layer contains the systems for high-level process supervision. For this task, com-

puters, networked data communications as well as graphical user interfaces are employed.

- **Programmable Logic Controller (PLC):** This layer contains small embedded systems controlling functional processes of manufacturing.
- **Sensors and Actuators:** The lowermost layer includes sensors and actuators which are usually interconnected by fieldbus systems. Sensor readings are taken by the PLCs which determines suitable actions for the actuators on the basis of the programmed logic.

The International Electrotechnical Commission (IEC) standardised industrial automation pyramid model (see IEC 62264 [7]) is still the baseline of modern industrial infrastructures. Characterised by isolation, restricted physical and digital access, this forms the foundation for tamper protection implemented in current industrial production sites.

2.2. Supply Chains

Throughout the years, the paradigm of labour division introduced an enhancement to the original approach of standalone industrial automation pyramids, coupling the independent production sites to complex supply chains.

The result of this development is illustrated by figure 3, where raw material suppliers provide their educts to the initial upstream producers. From these educts, upstream manufacturers create their intermediate products and forward them to the next upstream manufacturer. Combining all intermediate products supplied by upstream manufacturers, the final manufacturer on the supply chain creates the final product which is delivered to the customers. A good example for such a production chain is the automotive industry, where the final manufacturer assembles the car from the parts provided by contracted upstream manufacturers.

Each production plane illustrated in figure 3 represents an industrial pyramid which is connected to others through supply chains. To maintain the integrity of the whole supply chain, service providers take care of all necessary tasks like engineering, maintenance and management.

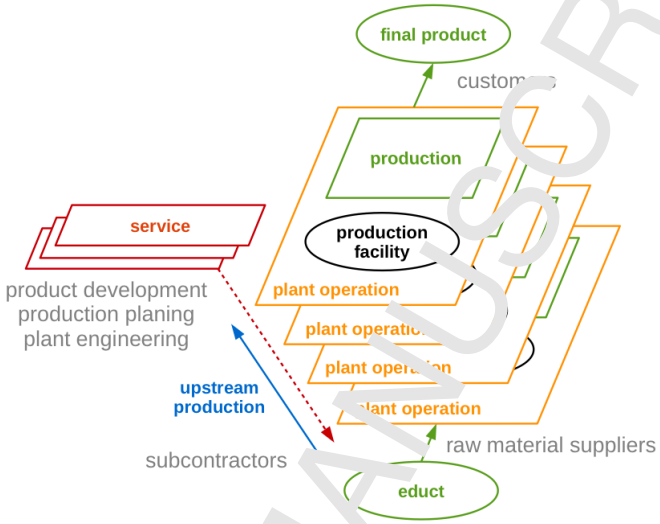

Figure 3: Simplified Model of Industrial Supply Chains (Adapted from [6])

In order to streamline manufacturing, the principle of labour division was continuously refined. Consequently, the number of intermediate products provided by subcontractors was raised continuously. To ensure reliable provision of necessary intermediate products, there was a demand to establish communication channels along the supply chains. Based on the concept of isolation, enhancement of the rigid industrial automation pyramid model with outbound communication channels is challenging.

Provided that these interactions are limited to the ERP level, implementation as well as maintenance of the corresponding interfaces can be conducted with an acceptable effort. As the major parts of the industrial automation pyramid remains segregated, process-data already known by the ERP can be provided without impairing isolation significantly. One prominent example for such interactions is just-in-time manufacturing which is the baseline of lean-production [7]. The complexity of the subjacent layers, however, makes it much more difficult to implement desired interactions without violating the paradigm of isolation.

Such connections might be required in cases where more detailed process-data should be provided in real-time to external requesters.

2.3. Remote Access Motivates Industrial Information Technology Security

Throughout the years, remote access to industrial facilities gained increased importance for lean-production and easy remote maintenance. Starting with small range serial Point-to-Point (PtP) connections in the 1960's, landline dial-up modems became the baseline for long range remote access during the 1970's. At the same time, Information Technology (IT) security became relevant for the first time in the history of industrial digitalisation.

Initially, the security of landline remote access was assured by a concept known as *Security by Obscurity*. The dial-in numbers to access corresponding industrial resources were kept secret but beyond that obscurity no additional IT security policies were implemented. Authentication methods such as passwords were often misunderstood as loss of privileges and caused increasing inconvenience. The fight of the free software movement founder Richard Stallman against passwords [8] in the mid 1980's is good evidence of this attitude. With the range of possible dial-in numbers high and the number of possible adversaries able to afford the costs involved in testing all possible numbers low, industry felt pretty secure.

Phreaking, as described in Bruce Sterling's book "The Hacker Crackdown" [9], soon proved *Security by Obscurity* an invalid security scheme for multiple reasons. The use of control in undisclosed audio frequencies enabled long-distance calls free of charge. Consequently, initially hypothetical brute-force attacks to secret dial-in numbers became feasible for adversaries with limited financial capabilities. Ironically enough, *Security by Obscurity* implemented by the landline operators enabled attacks on obscure dial-in numbers of industrial resources on a large scale. Finally, the availability of affordable computer systems in the 1980's, made *phreaking* popular. The Cold War computer espionage incident, where the German hacker Karl Koch was involved [10], is a good example of that development.

During all that time, the Advanced Research Projects Agency Network (ARPANET) continuously expanded by connecting information systems and finally evolved to the Internet, the name by which it is known since the 1990's [11]. Compared to connection-based landline PtP connections, Internet connections are packet-based and do not require dedicated communication lines per connection. Therefore, communication participants can easily eavesdrop all packets within reach.

While simple authentication methods resolved security issues of past PtP connections, the *CIA*-triad was introduced to mitigate threats emerging from packet-based connections. The *CIA* acronym used here is for *Confidentiality*, *Integrity*, and *Authentication*, indicating the three most important security assets of modern IT systems. Unlike simple password authentication of the past, *CIA* requires the use of cryptographic schemes. To keep these schemes effective, they also have to be periodically updated to the respective current state-of-the-art [12].

Due to the paradigm *Security by Isolation*, IT security of industrial environments was not investigated for a long time. Separation from the Internet and uniqueness of industrial sites seemed to be sufficient to reduce the likelihood of attacks [13]. Both assumptions have failed on a large scale in the recent past (cp. Stuxnet attack [14]) and lead to an increased interest in industrial IT and network security [15].

In contrast to IT security requirements of office environments, *Availability* of industrial assets is of high importance as production disturbance might result in significant financial losses. Therefore, the triad of security objectives is expanded to *CIAA* to be applicable to industrial facilities, where the second *A* is for *Availability*.

3 Arranging the Future

Current industrial facilities implement division of labour primarily in the field of rationalisation and utilisation of supply chains. Increased bandwidth for packet-oriented networks between different productions sites, however, enables

further development of division of labour on an infrastructural basis. Therefore, production machinery of future industrial sites is expected to get increasingly specialised and become part of frequently rearranged supply chains.

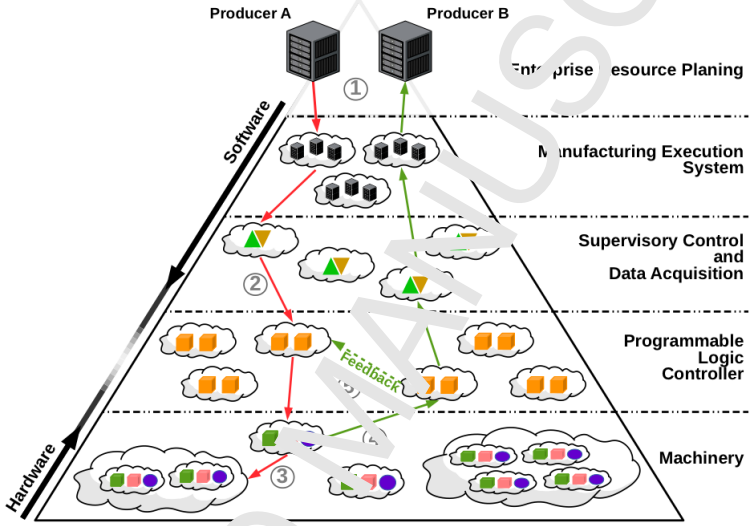

Figure 4: Decentralized Industrial Automation Pyramid

In figure 4 the authors introduce a model of a radical *all cloud approach* implementing the outlined infrastructural division of labour. The presented model enhances the classic industrial automation pyramid model introduced in section 2.1 and adds a decentralisation aspect novel for industrial infrastructures. As the layers of the classic model are still suitable to describe the basic architecture of industrial facilities, they are also used in the improved model. For the sake of simplicity, sensors and actuators are termed machinery. The factor of labour division is illustrated by clouds representing fractioned and specialised services. While services on top of the pyramid are software-oriented and virtualised by server clusters, the base remains hardware-oriented hosting real machines.

Compared to the classic model, production sites are virtualised and composed from fractioned services offered by different providers. The producer, illustrated on top of the pyramid in figure 4, determines the optimal combination of services

necessary for the respective production cycle. Thanks to the flexible model, adaptions of chosen combinations are possible at any time when cost optimisation or compensation for unavailable services is desired.

Figure 4 also outlines a simplified communication scenario for decentralised manufacturing, consisting of two producers A and B (see ①). In a wider context, both producers are part of a supply chain, where producer A manufactures upstream products for producer B. To form the virtual production-line, producer A determines the optimal service suppliers and establishes a path of decentralised communications (see ②). These dynamically established interconnections are used to distribute design files, status information or instructions between the interlinked services. Possible resource bottlenecks are resolved by the respective service providers themselves. Such an exemplary case is denoted by ③ in figure 4, where a service provider on the machinery layer is offloading workload to a subcontractor.

On completion of the actual workpiece, the machinery service provider notifies the service providers of the virtual production-line of producer B (see ④), where the manufactured upstream products are further processed. To improve the quality of the provided upstream products, it is feasible that service providers of different virtual production-lines share some feedback information on the same level of operation (see ⑤).

Besides aspects of logistics or standardised interfaces, communications and sufficient bandwidth are crucial for the proposed concept to succeed. Information exchange in an industrial setting will happen directly on machinery level. This will further increase the importance of secure and reliable machine-to-machine communication. To achieve a fully intergrated solution, like proposed in figure 4, hosted services need to be discoverable in an automated manner by the machines themselves. An broad overview on protocols to support service discovery is given in [16]. The standardisation of protocols and interfaces helps to develop compatible hardware and software solutions to ensure interoperability between operators and machines. The German *Plattform Industrie 4.0* consortium [17] proposes a Reference Architectural Model Industrie 4.0 (RAMI 4.0) [18] to

address some of these aspects. Both, the presented decentralised communications model as well as standardised RAMI 4.0 break up with the traditional *Security by Isolation* paradigm, which dominates industry for decades. Therefore, the topic of IT security plays an important role [19] for specification and implementation of future Industrial Internet of Things (IIoT) concepts which are also predicted by publications of the past [20]. Proven by experiences from the past (see section 2.3), neither deliberate ignorance nor implementation of anti-patterns such as *Security by Obscurity* are viable options to solve this challenge.

In the following sections of the paper, the aspects of decentralised industrial communications are investigated and categorised. Consequently, requirements for IT security are described. Finally, building blocks of security for the identified categories are provided.

4. Use-Cases of Decentralisation

Before essential security requirements for future decentralised IIoT infrastructures are introduced, some use-cases for the *all cloud approach*, presented in section 3, are provided. These are representative for typical industrial use-case scenarios and also the baseline for research within the scope of the "German reference project for IT security in context to Industrie 4.0" (IUNO) [21]. They also illustrate the usability of the presented decentralisation approach for real-world scenarios and aid the definition of significant IT security requirements for these infrastructures.

4.1. Virtual Manufacturing

The establishment of virtual manufacturing is beneficial to the sector in various ways. Two prominent variants, which are the focus of the IUNO project, are 1) the evaluation of manufacturability of customer individual products and 2) planning shopfloor production environments as virtual environments before they are implemented in reality.

Customers demand for more individualised products increases, which can be observed in industries like furniture manufacturing, where various combination

possibilities for kitchens or bath cabinets are demanded by the customers. In order to decide, whether a certain cabinet can be produced with the available machinery, production is evaluated using a virtual model of the machines on the shopfloor as well as a model of the requested product. These models are evaluated in a simulation to make parameters required for manufacturing plausible. With this step, possible shortcomings regarding the capabilities of the available machines can be determined. Furthermore, this analysis step is suitable to identify potential malicious settings which could harm production equipment and lead to loss of production and revenue.

As outlined in section 3, future machinery is likely to be even more specialised thus more expensive and an investor requires detailed analysis of planned shopfloor environments before they get build. Such planning is enabled by virtual manufacturing. Using models of the machines planned for the upcoming production sites shopfloor can help to identify bottlenecks ahead of time. Furthermore, processes of manufacturing or logistics can be simulated, and based on the machinery models the producible goods and possible quantities can be evaluated.

Depending on the detail level of the models and simulated environments, IT security related investigations and trainings can be conducted. Such a setting allows the study of real-world IT security incidents. It is possible to evaluate various strategies for mitigation, defence and protection without risking the real production equipment. With the identified findings the IT infrastructure of already deployed and newly planned sites can be further improved.

4.2. Technology Data Marketplace

Following the proposed division of labour, even on machinery level, production equipment should be well utilised in order to maximise revenues. In periods where free capacities are available, these can be offered to third parties. A practicable implementation of capacity allocation requires the implementation of a management platform which also addresses aspects of logistics and accounting.

These platforms can be also employed to implement a marketplace for different kinds of digital goods.

Different aspects of digital marketplaces are researched as part of the IUNO project. The researched use-case provides approaches for monetising manufacturing parameters often classified as secret intellectual property. An example of these parameters are instructions for the treatment of various raw materials processed by different cutting techniques such as water jet or laser cutting.

Additionally, topics like parameter licensing, data quality and data provisioning are researched. In the course of the research, secure availability was identified to be important. Therefore, a distributed infrastructure implementing the *CIAA* paradigm is also considered to be beneficial for this use-case.

4.3. Secure Remote Maintenance

Since the early times of landline dial up PtP connections, remote maintenance is a topic of interest. The advent of packet-oriented networks and the Internet as a globally accessible network has enabled novel use-case scenarios. As a consequence, remote connection devices are deployed on a large scale to be part of the Internet of Things (IoT), reducing the need for physical presence for machine maintenance or the acquisition of sensor readings.

To add convenience and accountability, remote maintenance is bundled with Ticket Request Systems (TRSs). These assign individual identifiers to each incoming case and help supporters and customers in progress tracking. Additionally, ticket systems are linked to certain remote connection devices, providing dynamic access for supporters.

Separated from public reach, it is supposed that remote maintenance services highly benefit from secure decentralised industrial infrastructures as these also foster interlinkage with third party components such as TRSs.

4.4. Visual Control Centres

Another challenge in the field of industrial control systems is the aggregation and visualisation of acquired data obtained from different sources. Virtual

dashboards refine such data for further inspection and help technicians to oversee critical process steps in manufacturing.

To enhance the benefit of these systems, anomaly detection algorithms as well as signature-based analysis of transferred data are introduced to form a Visual Security Control Centre (VSCC). Along with process supervision, the VSCC provides additional data for IT specialists to detect attacks on IT infrastructures.

The concept of secure decentralised industrial infrastructures improves data transfer which is the basis for traditional process monitoring. Especially, the option of outsourcing data processing to specialised third parties is seen as beneficial. Furthermore, the concept enables secure exchange of attack patterns between different participants of virtualised production lines such as introduced by figure 4 in section 3. Reaction time proved to be a good mitigation strategy in cases of attacks on infrastructures. Therefore, redundant availability of known attack patterns for VSCCs is seen as an additional benefit.

5. Requirements for Secure Infrastructures

In the preceding sections, a model for a radical decentralised industrial infrastructure was introduced and substantiated by industry use-case scenarios. In this section, the basic requirements for secure decentralised infrastructures are outlined which can considered as assets later on. Subsequently, dangers for these assets are examined using a threat classification model to identify vulnerabilities. From these, protection needs are determined and finally classified utilising the *CIAA* model.

Figure 5 presents all steps of the applied methodology. To cover a broad range of requirements for secure decentralised industrial infrastructures, figure 5 also contains a characteristical communication scenario adapted from figure 4. This scenario illustrates data exchange between participants of different virtual production lines beyond office and company boundaries posing new technical challenges. Considering the outlined use-cases from section 4, five generic requirement categories have been identified.

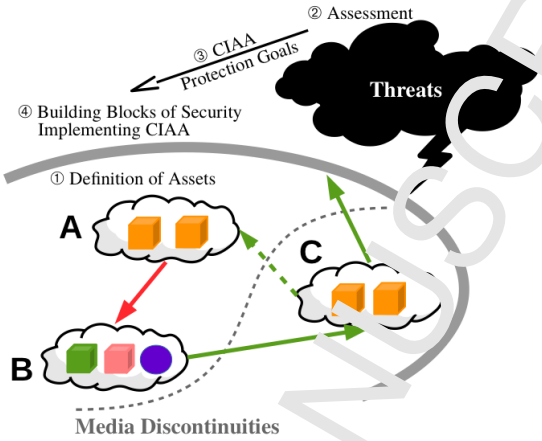

Figure 5: Methodology Determining Security Requirements

The requirement categories as well as the results of the corresponding security assessments are the basis for the elaborated building blocks of security.

5.1. Use-Case Asset Definition

From evaluation of the communication scenarios described in section 3 and the use-cases introduced in section 4, important assets have been developed. In order to maintain the integrity of a virtual production line, these assets have to be maintained by protecting them against attacks.

5.1.1. Secure Data Transfer

Assuming that all communication participants of a virtual production line are situated at separated locations, secure communication schemes are mandatory. As decentralised infrastructures replace fixed structures with dynamic ones, the concept of End-to-End (E2E) security plays an important role. Eliminating zones of trust which are typical for current industrial networks, each entity of the decentralised infrastructure has to ensure secure data transfer.

5.1.2. Connection Establishment

Because of the absence of fixed network infrastructures, topics of secure network discovery and identification of valid communication participants are crucial. Besides dynamic routing, the issue of bypassing restrictions of underlying networks are important.

5.1.3. Identity Management

Coordinating flexible lines of production requires secure options for registration, authentication and management of communication participants. This also involves secure storage and management of required authentication credentials.

5.1.4. Data Processing

For each of the presented use-cases, secure processing of data is important. Since data is produced by various sources and transmitted via different networks, aggregation and storage is a challenging task. Enabling provisioning of all nodes associated to a virtual production line with manufacturing data, repositories have to be implemented. Due to the decentralised approach, the data has to be processed to match the requirements of the respective use-case. One example is the disaggregation of huge data blocks in order to realise redundant provisioning. For this reason, the identification of data chunks also plays an important role in data processing. Additionally, post-processing could also be enriched with adaptive schemes for plausibility testing of received data to minimise risk of malfunctions.

5.2. Threat Assessment

For identification and quantification of possible threats for the outlined assets, the *STRIDE* [22] classification model is employed. For this approach, the following threats are considered to be of importance:

- **Spoofing:** Any violation of authenticity. Attacks include message spoofing or forged communication partners.

- **Tampering:** Any violation of integrity. Attacks include alteration, replay or malformation of messages or data.
- **Repudiation:** Threats for the transparency of actions, resulting in unlinkability of events to their cause.
- **Information Disclosure:** Any violation of confidentiality. Attacks include eavesdropping and also the use of forged communication partners.
- **Denial of Service:** Illegitimate blocking of services by third parties. Usually, Denial of Service (DOS) is initiated by resource starvation of available bandwidth, computation power or memory.
- **Elevation of Privilege:** Increasing privileges for an entity through manipulations or bypassing.

STRIDE defines the following abstract standard assets:

- **Processes:** Computing resources used for data processing.
- **Data Stores:** Resources utilised for permanent or temporary data retention.
- **External Entities:** Systems not controlled by the respective object of investigation. This includes remote communication partners, such as remote computer systems, but involves also Human to Machine Interaction (HMI).
- **Data Flows:** Transmission of data between entities.

The concept of trust boundaries is completing the *STRIDE* model. Within one trust boundary, the level of confidence in security is the same, as an attacker needs the same effort to access any system within this boundary.

Therefore, one suitable technique in determining threats is data flow analysis. Whenever the data flow is crossing a predefined boundary, emerging threats can be identified and recorded for subsequent evaluation. Substantiated by expert

knowledge and literature [12], each of the introduced standard assets can be correlated to characteristic threats of the *STRIDE* model. Taking this experience into account, typical correlations between standard assets and threats can be summarised as shown by table 1.

Table 1: Correlation of *STRIDE* Standard Assets and Threats

Threats \ Standard Assets	Process	Data Store	External Entities	Data Flows
Spoofing	✓		✓	
Tampering	✓	✓		✓
Repudiation	✓	✓	✓	
Information Disclosure	✓	✓		✓
Denial of Service	✓	✓		✓
Elevation of Privilege	✓			

To obtain comparable results from the analysis, the use-case assets from section 5.1 are mapped to the introduced standard assets of this section. As the use-case assets combine different application scenarios, they cannot simply be matched to one specific standard asset counterpart. Multiple standard assets have to be assigned to each of the use-case assets in order to outline the complete picture. The results are shown by table 2.

A good illustration of this course of action is the use-case asset Secure Data Transfer which is comprising not only the application scenario data transfer, but also authentication of involved communication peers. To cover all possible threats for the considered scenarios, Secure Data Transfer has been linked to the *STRIDE* standard assets External Entities and Data Flows.

In the following section, general IT security protection objectives are introduced. These are associated to the use-case asset classes and the basis for identifying mitigations for the threats summarised by table 2.

Table 2: Mapping of Use-Case Assets to *STRIDE* Standard Assets

Use-Case Assets \ Standard Assets	Processes	Data Stores	External Entities	Data Flows
Secure Data Transfer			✓	✓
Connection Establishment			✓	✓
Identity Management		✓	✓	
Data Processing	✓	✓		

5.3. IT Security Protection Objectives

To qualify IT security protection needs, literature [23] specifies a set of protection objectives which are commonly accepted. In practice, each objective has corresponding building blocks of security implementing the respective protection.

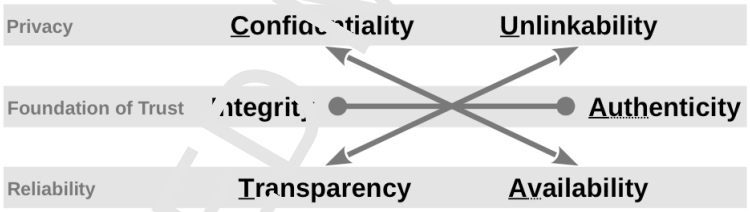

Figure 6: IT Security Protection Objectives

Figure 6 illustrates these objectives ordered by the role they play in IT security. The centre of secure systems is formed by the foundation of trust consisting of Integrity combined with Authenticity. Measures of Integrity protection ensure that data corruptions can be detected while Authenticity assures that the source of data is known and trusted.

Although, technical implementations of Authenticity always requiring Integrity for data and cryptographic keys, separation of both terms is reasonable. As the foundation of trust is implemented utilising building-blocks from both categories, it is crucial to employ a significant terminology to address these pre-

cisely. Furthermore, in some industrial use-cases, Integrity is applied standalone when just data protection is desired.

The diagonally opposite objectives of the remaining group Privacy and Reliability, are contradicting each other. Therefore, it is not possible to satisfy them at the same degree if both are to protect a specific asset. A sharp contrast is the relation of Transparency and Unlinkability. While Transparency requires data recording and retention for continuous analysis, Unlinkability demands data minimisation facilitating privacy. The same applies for Confidentiality and Availability, as encryption misconfigurations might render critical process-data unreadable.

Table 3: Correlation of Assets to IT Security Protection Objectives

Standard Assets / Use-Case Assets	Processes	Data Stores	External Entities	Data Flows
Secure Data Transfer			**Auth**	**C, I, Av**
Connection Establishment			**Auth**	**I, (C)**
Identity Management		**I, Auth, C, Av**	**I, Auth**	
Data Processing	**Auth, Av, I, T**	**Av, I, C, T**		

To identify the need for action, the IT security protection objectives of figure 6 are assigned to the Assets outlined by table 2. The result is shown by table 3 where the objectives are listed in their decreasing order of importance. As the topic of Transparency is considered to be paramount for industrial use-cases, the objective Unlinkabiltiy was not considered in table 3 and is also not further evaluated.

6. Safeguarding Decentralised IoT Structures

Section 5 specified the security requirements for the decentralised industrial infrastructures outlined in section 3. Taking the identified IT protection objectives of table 3 into account, this section presents methods for safeguarding the corresponding assets.

6.1. Building-Blocks of Security

To implement measures satisfying the generalised IT security protection objectives stated in section 5.3, the *state-of-the-art* provides distinct building blocks. These can broadly be classified into the categories *Primitives* and *Protocols* which are utilised to secure *Applications*.

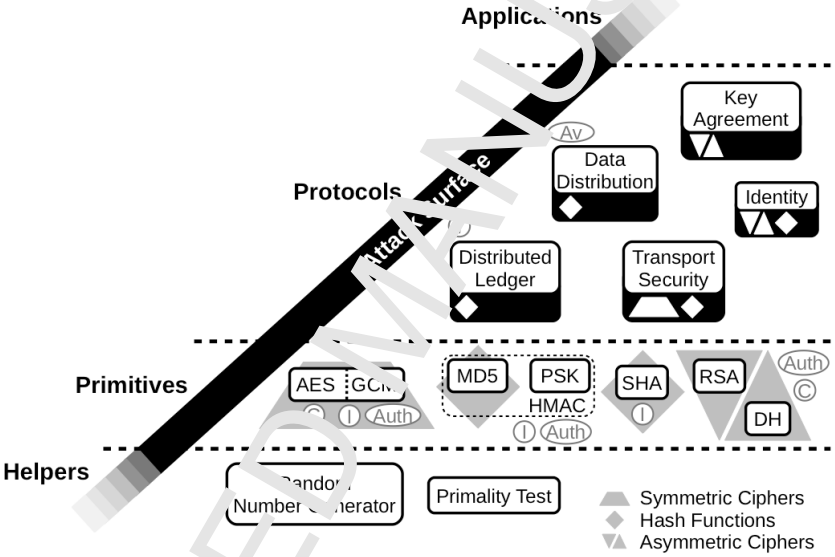

Figure 7: Relation of Protocols to their Corresponding Primitives

The primitives can be considered to be the smallest element of a security implementation. Based on cryptographic methods, these are the basis for Confidentiality, Integrity and Authenticity. Figure 7 introduces common used methods and shows some of their practical implementations.

In applications where Confidentiality should be established while consuming only little system resources, Symmetric Ciphers are used. Though, small hardware requirements are beneficial for embedded platforms, all participants are required to share the same cryptographic key which is referred to as Pre-Shared-Key (PSK). This introduces an overhead in key management and distribution which

is often seen as a drawback for the ease of use. Figure 7 introduces the Advanced Encryption Standard (AES) as a well-known representative of this class of ciphers. Some of the available Symmetric Ciphers also support different modes, enhancing the provided level of protection and targeting additional protection objectives. A good example is the Galois/Counter Mode (GCM) of AES also contributing Integrity and Authenticity to the protection.

To protect data Integrity and make information uniquely identifiable, cryptographic Hash Functions are employed. These are one-way functions, generating an unique string of fixed length known as fingerprint from an arbitrary amount of input-data. As the unique string exactly maps to the respective input-data, it is called a *Digest*. An important design goal of Hash Functions is a high degree of collision resistance, which means that similar input-data leads to the creation of Digests differing significantly from each other.

One-way function and collision resistance makes Hash Functions also interesting for authentication purposes as it is used by Keyed-Hash Message Authentication Codes (HMACs) [24].

Finally, there is the family of Asymmetric Ciphers which is based on the principle of public-key cryptography [25] and providing basic building blocks for Authenticity and Confidentiality. As these schemes are resource demanding, they are often used together with other cryptographic primitives as part of hybrid schemes. The security of the commonly employed Asymmetric Ciphers rests on two mathematical problem classes. The first class is based on Prime Factorisation (PF) for big numerical values and is the foundation of the Rivest-Shamir-Adleman (RSA) public-key cryptosystem. The second class utilises the difficulty of finding the Discrete Logarithm (DL) [26] for certain mathematical groups. It is the basis for establishing secret keys via a public communication channel and denoted as Diffie-Hellman (DH) key exchange. Apart from advances in research solutions for these mathematical problems, improvements in computation power pose a great risk for these ciphers. As a consequence, the recommended key-lengths (see [27]) are increased constantly in order to retain security of currently used

schemes for a predictive period of time. Additionally, alternatives also known as post-quantum cryptographic functions [28], are researched.

To utilise the introduced cryptographic primitives for their use in applications, they are joined together by cryptographic protocols. Some real use-case application examples are illustrated by figure 7. In all of these examples, the basic CIA protection relies on the reliability of the underlying primitives. Therefore, an important design goal of protocols is interchangeability of certain cryptographic functions to enable fallback scenarios and support cryptographic agility. As explained on the example of Asymmetric Ciphers, also the length of cryptographic keys has to be adjustable and comply with the recommendations of reputable institutes.

Analogous to the relation of the introduced primitives to their respective protection objective, complex use-case scenarios split into small function-blocks. One example for that issue is the use case "communication", which can be considered to be composed of function-blocks for Key Agreement, Identity and Transport Security. Following that scheme, the well-known Transport Layer Security (TLS) protocol [29] is labeling the ciphers which are used by the particular cipher-suites.

While the function-blocks of secure communication use-cases inherit their CIA properties from the employed primitives, the remaining security objectives Availability and Transparency are implemented on the protocol layer itself. To achieve this, suitable primitives are combined with other necessary methods.

An example for protocols implementing Transparency are Distributed Ledgers [30]. These are linked lists where sets of transactions are recorded in a chronological sequence. These sets are called blocks and are continuously synchronised with all participating peers. The complete history of all relevant blocks is known by all peers representing a log of all transactions enabling Transparency. Hash functions are employed to guarantee the integrity of all log entries. To prevent an attacker from recreating complete transaction logs with falsified data, the prerequisite of a successful recording is a proof-of-work to a resource consuming cryptographic challenge. One well-known practical example for an implementa-

tion of Distributed Ledgers are the various cryptographic currencies whose base technology is broadly known as Block Chain [31].

Implementations of Availability are following the same principle. One valid approach to guarantee this protection goal is to generate data redundancies provided by several computer systems. To streamline that process, data slices are created and made uniquely identifiable through the creation of Hash Function Digests. The data slices are deployed to their decentralised infrastructure which is able to track them by their Digests.

Because of its complexity, the majority of the codebase is utilised for the protocol functions. Taking also into account that program code of the protocol layer is the first instance processing data received from external sources, protocols seem to be more susceptible to attacks than particular primitives. Therefore, specification and development of new security protocols requires subtle and cost intensive testing throughout the whole product life-cycle to detect serious mistakes [32]. Also, for this reason, only proven cryptographic primitives should be used and unnecessary reinventions avoided [33].

To enable small and mid sized enterprises participation, one requirement for future decentralised industrial infrastructures is reuse of existing technology where it is suitable. In this context, the use of Free and Open Source (FOS) is seen to be highly beneficial as access to specifications and source code enables security audits as well as intensive testing for interested parties.

6.2. A Brief Outline of Promising Free and Open Source Approaches

In this section, a set of promising FOS tools and their baseline protocols are introduced. In the course of the research, these have been identified as suitable building-blocks for an implementation of future decentralisation scenarios such as outlined in section 4. Table 4 provides an overview of these tools and illustrates where they help safeguarding the Use-Case Assets defined in section 5.1. Finally, table 5 gives a summary of the underlying security protocols for each tool and maps them to the IT security protection objectives stated in section 5.3.

Table 4: Tools Mapped to Use-Cases Assets

Tools \ Use-Case Assets	Secure Data Transfer	Connection Establishment	Identity Management	Data Processing
BitTorrent		✓		✓
WireGuard	✓	✓		
BorgBackup	✓			✓
Syncthing	✓	✓	✓	✓
TOR	✓	✓		
B.A.T.M.A.N.		✓		
NetBSD Syslogd	✓			✓
The Tangle				✓

Invented by Bram Cohen in 2001, the BitTorrent protocol is the first and oldest practical implementation of a distributed Peer-to-Peer (P2P) file sharing protocol. Because of its age, it also inspired other FOS projects implementing elements of decentralisation. Currently, the advancement of the protocol is coordinated by BitTorrent Enhancement Proposals (BEPs) [34] where proposals and specifications of new features are assigned unique numbers. According to the initial protocol specification, files are split into chunks which are made uniquely identifiable by cryptographic hash values. Whenever a file is shared by a peer, these hash values and additional metadata are provided to a central service which is called tracker. Maintaining the metadata the tracker acts as a directory for all shared files which can also be queried by other peers. As every communication participant acts also as a server for all received chucks, the tracker is regularly updated with such metadata by all participating peers. Identified the tracker as a single point of failure threatening the Availability of the evolved P2P swarm, a BEP specifying Distributed Hash Tables (DHTs) was made. With this enhancement, the peers keep track of all metadata themselves. Therefore, the tracker is only crucial during the connection phase of a peer for initial metadata bootstrapping. Enhancing the scalability of the established P2P swarm, another BEP specifies use of multiple trackers which turned out to be ineffective compared to the DHT approach [35]. Addressing file sharing, Confidentiality

and Authenticity are not primary protection goals. Nevertheless, BEP-35 drafts a signature method to verify the Authenticity of a torrent issuer. The topic of Confidentiality is targeted by BEP-08 proposing some weak obfuscation. As this scheme turned out not to be very effective so far, Confidentiality is still left to underlying secure transport protocols such as Virtual Private Networks (VPNs).

Ensuring secure communications on the transport layer in terms of Confidentiality, Integrity and Authenticity, various FOS as well as proprietary solutions are available. Implementing future decentralised industrial IoT infrastructures, especially the FOS WireGuard (WG) [36] VPN provides a set of promising approaches. On the basis, WG employs the Noise Protocol Framework [37] which is a solid foundation implementing Confidentiality, Integrity and Authenticity. The verification of remote peers rests on asymmetric public-key cryptography and Public Key Pinning (PKP). Therefore it is possible that secure authenticated connections are established automatically. Adding to the resilience of the protocol, session cookies were implemented making DOS attacks harder. With session cookies, any initial connection is linked to a cryptographic challenge the peer has to solve. Since the proof-of-work is a prerequisite for a successful handshake, the risks of DOS attacks resulting in resource starvation are effectively mitigated. As the aspect of performance is one of the key development objectives, WG is implemented as a Loadable Kernel Module (LKM) for the Linux Operating System reducing significantly the overhead in Userspace/Kernelspace interaction. This aspect and less resource consuming cryptographic primitives make this VPN interesting for embedded IoT appliances. Compared to well-established standards like Internet Protocol Security (IPsec), WG enables simple setup and is based on a simple design consisting of less than 4,000 lines of code. The latter aspect also allows formal verification of the codebase which is currently being conducted [38].

Utilising the file chunking approach also known from BitTorrent, BorgBackup [39] implements a backup solution from this technology. Efficiently utilising the storage, BorgBackup performs a deduplication on chunk-level. From an IT security point of view, the software provides encryption capabilities ensur-

ing Integrity as well as Authenticity for the data. In cases of backup distribution or remote updates, the Secure SHell (SSH) protocol [40] is used for transport security.

While BitTorrent implements an unrestricted swarm file sharing among self-organised P2P nodes, the Syncthing [41] specification realises a secure decentralised file storage used for community clouds. Basically, Syncthing is used to keep files synchronised on different authorised systems. Analogous to BitTorrent, subprotocols are specified for the different IT security protection objectives. On the basis, anonymous TLS is employed for Confidentiality and Integrity. The Syncthing Block Exchange Protocol (SBEP) is responsible for the complete data processing and the authentication of connecting peers. For efficient transmission, files are partitioned into chunks which can also be requested separately by authorised peers. For authentication, the SBEP layer receives the asymmetric cryptographic authentication fingerprint obtained from the anonymous TLS handshake. Verifying the privileges of a connecting peer, the SBEP is performing a lookup on a list of a locally saved PKP table. If the received fingerprint is listed with sufficient permissions, access is granted by the SBEP. Implementing Availability, two protocols are provided. Detecting Syncthing shares on local networks, periodical checks are performed by the Syncthing Local Discovery Protocol. Shares which are not available on local networks are found by the Syncthing Global Disovery Protocol where a directory server maintains the status of all participating Syncthing instances. In cases where access between two Syncthing instances is blocked by a firewall, the Syncthing Relay Protocol enables the communication through an intermediate server. Since the relay server is acting as a TLS proxy, the E2E security is also maintained in such scenarios.

As stated in the previous sections, the IT security protection objective, Unlinkability, does not play an important role in industrial infrastructures.

For the sake of completeness and because of its interesting distributed networking approach, the The Onion Router (TOR) [42] is worth mentioning. To enable privacy, data traffic between two peers is relayed through a cascade of

nodes which ensures that its origin gets anonymised. To avoid information disclosure in the course of the relaying process, the traffic between the peers gets encrypted following an onion-model scheme. Implementing the concept of distributed networking eliminates the problem of single point of failure in network organisation. Hence, protocols such as TOR are also potentially interesting candidates in the efforts to enhance Availability.

Another approach of distributed networking are ad hoc mesh network protocols such as the proprietary Institute of Electrical and Electronics Engineers (IEEE) standard 802.11s. Initially developed for Wireless Local Area Networks (WLAN), FOS implementations like *Better Approach To Mobile Ad-hoc Networking advanced (B.A.T.M.A.N.)* are also used to employ existing Wide Area Networks (WANs) as a basis for establishing and maintaining separate decentralised networks. A good practical example where scalability of distributed networking is also researched are the networks operated by the German Freifunk movement [43]. Since ad hoc networks should allow unrestricted meshing of all participating nodes, topics of Authenticity are mostly not covered by the respective specifications. For the B.A.T.M.A.N. protocol, the BatCave extension [44] proposes a node authentication approach.

For future industrial decentralised applications, topics of accountability will be of high relevance. Enabling Transparency, the topic of secure logging is of importance. Since some potential adversaries have also access to the raw log files, maintaining the integrity of once authenticated entries is challenging. For cases where logs must be kept locally, the Request for Comments (RFC) standard 5848 [45] specifies a scheme which is also known as syslog-sign and found as a secure portion of the NetBSD [46] version of Syslogd. Compared to other approaches, its theoretical foundations [47] are quite mature and have been refined constantly. Therefore it is considered to be a capable candidate satisfying the IT security protection objective Transparency.

If distribution of logged information is a feasible approach for a certain application scenario, Distributed Ledgers are a valid option to establish Transparency. Addressing also the issue of small embedded systems which are typical

for industrial manufacturing infrastructures, *The Tangle* [48] provides a scheme for the implementation of a resource friendly but secure Distributed Ledger. Compared to other protocols like Bitcoin, The Tangle is not based on fees which is obsoleting powerful authorities required for the authentication of new entries. To make a valid transaction, a peer has simply to validate two randomly selected transactions which are recorded in a Direct Acyclic Graph (DAG) forming a tangled structure. One benefit of this structure is, that sub-tangles can also be temporarily detached and operated from the main-tangle, enabling off-line transactions. This feature and the use of DAGs adds to scalability of the system. While the technology has been open sourced, the non-profit IOTA foundation maintains an ecosystem which can actually also be used for micro-payments. Fostering industrial use-cases, the IOTA foundation also currently collaborates with industrial partners. The name IOTA itself is not referring to an acronym [49] as it would be guessed first, but to the ninth letter of the Greek alphabet. Since the expression "not one iota" (cp. the Bible, Matthew 5:18) also refers to very small amounts, the term IOTA also underpins the intended relevance for micro-payments.

Table 5: Open Source Tools Mapped to IT Security Protection Objectives

Tools / *Underlying Protocols* \ Protection Objectives	C	U	I	Auth	T	Av
BitTorrent						
BEP-03: BitTorrent			✓			✓
BEP-05: DHT						✓
BEP-08: Obfuscation	✓					
BEP-12: Multi Tracker						✓
BEP-35: Torrent Signing			✓	✓		
WireGuard						
Noise Protocol Framework	✓		✓	✓		
Session Cookies						✓
BorgBackup						
SSH	✓		✓	✓		
Borg-RPC	✓		✓	✓		✓
Syncthing						
TLS	✓		✓			
Bock Exchange Protocol			✓	✓		
Global Discovery Protocol						✓
Local Discovery Protocol						✓
Relay Protocol						✓
TOR						
Onion Routing	✓	✓	✓			
B.A.T.M.A.N.						
Batman Protocol			✓			✓
BatCave Proposal			✓	✓		
NetBSD Syslog						
TLS	✓		✓	✓		
Syslog-sign			✓	✓	✓	
The Tangle						
Direct Acyclic Graph			✓	✓	✓	
Distribution						✓

This section provided an overview of some promising protocols currently developed and implemented by several FOS communities. Although, none of the presented tools at their current development state is able to implement the complete model architecture of section 3, the presented core-technologies represent a good starting point for an implementation of secure decentrialised future industrial IoT infrastructures based on FOS tools.

Summary

This work summarises the technological progress of industrial IoT up to the present day. Familiarising with the concept of division of labour, the impacts of the additional forces mechanisation and digitisation on manufacturing processes were introduced. In essence, the whole progress can be expressed by the model provided by figure 1 where the axes illustrate the progress of the identified forces over time. It is assumed, that creation of each of the axes originates from events which are also referred to as industrial revolutions [5]. Especially digitisation affected modern manufacturing very much and led to the establishment of hierarchies resulting in well and tightly organised supply chains as illustrated by figure 3.

These links identified so far, served as starting point allowing an estimation for the future. A model of a decentralised industrial IoT based upon expected future requirements is presented in section 3. The developed result is denoted as *all cloud approach* and illustrated by figure 4.

Even though the outlined model is considered to be more a subject of future development, there are real world use-cases derived from current research projects provided in section 4 which will benefit from such an environment. As the introduced scenario requires sustainable changes of the associated manufacturing processes, possible threats and mitigation strategies have to be considered first.

Consequently, the provided real-world use-cases served as a basis to derive the use-case specific assets of section 5.1. By applying the well-established STRIDE threat analysis on them, corresponding threats were identified. Correlating these with the use-case assets the corresponding IT security protection objectives are derived and provided by table 3. The result forms the starting point for selecting suitable combinations of security mechanisms to mitigate the identified threats.

Finally, section 6 presents a systematic foundation to show how the identified security requirements can be addressed by technical actions. Open Source projects are suggested as an appropriate solution to face these challenges. Adapting

proven methods from established open source projects aids establishing a reliable and economical future manufacturing environment.

Conclusions and Future Work

In this work two models were developed and presented. The first one is illustrated by figure 1 and arranges technological and organisational aspects to the context of the evolution of industrial manufacturing. From this model it was concluded, that the current developments in industrial IoT cannot be viewed as groundbreaking new. Following the path of these findings, those new developments are seen as further development of division of labour in combination with digitisation. Continuing this thought and incorporating the current state of industrial manufacturing and associated future requirements, a model describing a likely future industrial manufacturing environment was developed and introduced in figure 4. Concluding the results so far, current developments in industrial manufacturing are not seen as groundbreaking and denoting them as a 4th industrial revolution is not justifiable as it is often argued by certain parties. The sum of all steps, however, is heading in that direction and forms the basis for the next pending technical revolution.

In each phase towards that direction, IT security is an essential component establishing and maintaining integrity of industrial manufacturing environments. As it is expected that future industrial facilities will be mesh-worked, IT security provides the anchor to facilitate safeguarding functional safety features. All these aspects require that IT security is not be seen as just a minor aspect of product development. It rather has to be treated as a process supporting the product lifetime avoiding mistakes known from other IoT domains (e.g. [51] and [52]). To address these challenges, proven solutions from other domains such as office IT can be transferred and this will provide a good starting point. Adjustments to these solutions, however, must address the specific requirements of industrial manufacturing.

Investigating the feasibility of knowledge transfers to the industrial domain, history tells us that such approach is not uncommon. Demonstrated by the adaption of early computer science findings initially developed for the purposes of WWII [4], novelties are regularly adapted for industrial manufacturing, but sometimes with a significant delay. It turns out, that the driving factor for these improvements is often not their innovation aspect, but efficiency enhancement resulting in cost reductions or legal requirements.

Beyond the technical viewpoint, the outlined development can influence other domains. As seen from the past developments, disruptive changes in the technical world also affect economy and society. Therefore, another task of future research is to investigate the effects of progressing digitisation and radical division of labour on society and related coping strategies [53].

The key idea behind the presented work is to use available and proven components whenever possible to master the industrial IT security challenges ahead. The basic approach was demonstrated on a future manufacturing environment consisting of inter-meshed facilities. Addressing the expected increasing complexity security minded development strategies and following the paradigm *Security by Design* are seen to be important. Even though these might not be applicable to existing legacy systems, newly designed systems and environments should consider a proper security design and maintain agreed security standards throughout the complete lifetime of the respective devices.

In conclusion, IT security is not a product [54] and will never become one. Ensuring reliability and IT security throughout the complete lifetime of operation, life cycle management processes have to be defined, maintained and pursued. To be effective these processes need to be continuously reviewed to reflect the particular state-of-the-art and must also be applied by associated subcontractors.

This paper provided a look into a probable future of industrial manufacturing and summarised challenges as well as possible open source solutions for associated IT security issues. To identify opportunities resulting from possible technology transfer, upcoming research has to focus on interdisciplinary collaboration between IT security specialists and experts of the respective domains. This is seen

as an important key factor in developing sustainable, secure and cost efficient future designs.

Project Funding

The presented work is part of the German national IT security reference project *IUNO* [21] which is funded by the German Federal Ministry of Education and Research under Grant № KIS4ITS0001. *IUNO* aims to research and provide building-blocks for IT security in the emerging field of Industrie 4.0. The work is also partially supported by the Science Foundation Ireland Smart Manufacturing Centre, *Confirm* [55], under Grant № 16/RC/3918.

References

[1] Adam Smith, An Inquiry into the Nature and Causes of the Wealth of Nations, University of Chicago Press, 1776.

[2] Karl Johan Åström, Bjorn Wittenmark, Computer Controlled Systems – Theory and Design, Prentice Hall, 1997.

[3] Gartner Research Analyst Noha Tohamy, Hype Cycle for Supply Chain Strategy (2017).
URL https://www.gartner.com/doc/3765865

[4] Michael Pöse, Chiffriermaschinen und Entzifferungsgeräte im Zweiten Weltkrieg - Technikgeschichte und informatikhistorische Aspekte (German), Ph.D. thesis, Technical University Leipzig (2004).

[5] ISO, IEC 62264-1:2013 Enterprise-control system integration - Part 1: Models and terminology (2013).
URL https://www.iso.org/standard/57308.html

[6] VDI/VDE, Industrie 4.0 Statusreport – Wertschöpfungsketten (2014).
URL https://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/sk_dateien/VDI_Industrie_4.0_Wertschoepfungsketten_2014.pdf

[7] T. Ohno, The Toyota Production System Beyond Large Scale Production, CRC Press, 1988.

[8] S. Williams, Free as in Freedom – Richard Stallman's Crusade for Free Software, 2nd Edition, Free Software Foundation, 2010. doi:10.1109/MSPEC.2002.1049262.

[9] B. Sterling, The Hacker Crackdown: Law and Disorder on the Electronic Frontier, Bantam Books, Inc., New York, NY, USA, 1992.

[10] Der Spiegel, Hacker aus Hannover und Berlin spionierten für das KGB durch Dutzende amerikanischer Computer-Systeme (1989).
URL http://magazin.spiegel.de/EpubDelivery/spiegel/pdf/13493011

[11] Barry M. Leiner et al., A Brief History of the Internet, ACM SIGCOMM Computer Communication Review (2009) 22–31Volume 39 Issue 5. doi:https://doi.org/10.1007/978-3-642-13247-6_1.

[12] M. Howard, S. Lipner, The Security Development Lifecycle, Microsoft Press, Redmond, WA, USA, 2006. doi:10.1007/s11623-010-0021-7.

[13] V. M. Igure, S. A. Laughter, R. D. Williams, Security issues in SCADA networks, Computers & Security 25 (2006) 498–506. doi:10.1016/j.cose.2006.03.001.

[14] Ralph Langner, To Kill a Centrifuge – A Technical Analysis of What Stuxnet's Creators Tried to Achieve (2013).
URL https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

[15] S. Luque Anton, D. Fraunholz, C. Lipps, F. Pohl, M. Zimmermann, H. D. Schotten, Two Decades of SCADA Exploitation: A Brief History, in: Conference on Applications, Information and Network Security (AINS), Malaysia, IEEE, 2017. doi:10.1109/AINS.2017.8270432.

[16] B. C. Villaverde, R. D. P. Alberola, A. J. Jara, S. Fedor, S. K. Das, D. Pesch, Service discovery protocols for constrained machine-to-machine communications, IEEE Communications Surveys Tutorials 16 (1) (2014) 41–60. doi:10.1109/SURV.2013.102213.00229.

[17] Platform Industry 4.0 Consortium, Plattform Industrie 4.0 (2017).
URL http://www.plattform-i40.de

[18] VDI/VDE, Status Report: Reference Architecture Model Industrie 4.0 (2015).
URL https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/GMA_Status_Report_-_Reference_Archtitecture_Model_Industrie_4.0__RAMI_4.0_/GMA-Status-Report-RAMI-40-July-2015.pdf

[19] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of things security and forensics: Challenges and opportunities, Future Generation Computer Systems 78 (P2018) 544 – 546. doi:https://doi.org/10.1016/j.future.2017.07.060.
URL http://www.sciencedirect.com/science/article/pii/S0167739X17316057

[20] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems 29 (7) (2013) 1645 – 1660, including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications — Big Data, Scalable Analytics, and Beyond. doi:https://doi.org/10.1016/j.future.2013.01.010.
URL http://www.sciencedirect.com/science/article/pii/S0167739X13000241

[21] IUNO Project, German National Reference Project for IT Security in Context to Industrie 4.0 (IUNO) (2018).
URL https://www.iuno-projekt.de

[22] Microsoft, The STRIDE Threat Model.
URL https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[23] Claudia Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle (German Edition), De Gruyter Oldenbourg, 2014.

[24] IETF, RFC 2104 – Definition of HMAC
URL https://tools.ietf.org/html/rfc2104

[25] W. Diffie, M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory 22 (6) (1976) 644–654. doi:10.1109/TIT.1976.1055638.

[26] S. M. Kevin, The discrete logarithm problem, Cryptology and computational number theory 42 (1990) 49

[27] BSI, TR-02102-1 – Kryptographische Verfahren: Empfehlungen und Schlüssellängen.
URL https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[28] R. Niederhagen, M. Waidner, Practical Post-Quantum Cryptography, Tech. rep., Fraunhofer SIT (08 2017).
URL https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Practical.PostQuantum.Cryptography_WP_FraunhoferSIT.pdf

[29] E. Rescorla, T. Dierks, The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246 (Aug. 2008). doi:10.17487/RFC5246.
URL https://tools.ietf.org/html/rfc5246

[30] L. D. Ibáñez, E. Simperl, F. Gandon, H. Story, Redecentralizing the web with distributed ledgers, IEEE Intelligent Systems 32 (1) (2017) 92–95. doi:10.1109/MIS.2017.18.

[31] Arshdeep Bahga and Vijay K. Madisetti, Blockchain Platform for Industrial Internet of Things, Journal of Software Engineering and Applications 9 (10) (2016) 533–546. doi:10.4236/jsea.2016.91036.

[32] Christopher Meyer, 20 Years of SSL/TLS Research – An Analysis of the Internet's Security Foundation, Ph.D. Thesis, Ruhr-University Bochum (2014).
URL http://www-brs.ub.ruhr-uni-bochum.de/netahtml/HSS/Diss/MeyerChristopher/diss.pdf

[33] B. Schneier, Cryptography: the importance of not being different, Computer 32 (3) (1999) 108–109, 11. doi:10.1109/2.751335.

[34] B. Cohen, The bittorrent protocol specifications (2013).
URL http://bittorrent.org/beps/bep_0000.html

[35] G. Neglia, G. Reina, H. Zhang, D. Towsley, A. Venkataramani, J. Danaher, Availability in BitTorrent Systems, in: IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications, 2007, pp. 2216–2224. doi:10.1109/INFCOM.2007.256.

[36] J. Donenfeld, WireGuard: Next Generation Kernel Network Tunnel, in: Proceedings of the 2017 Network and Distributed System Security Symposium, NDSS'17, San Diego, USA, 2017. doi:10.14722/ndss.2017.23160.
URL https://www.wireguard.com/papers/wireguard.pdf

[37] Trevor Perrin, The Noise Protocol Framework Specification (Rev. 33) (2017).
URL http://noiseprotocol.org/noise.pdf

[38] J. Donenfeld, K. Milner, Formal verification of the wireguard protocol (July 2017).

URL https://www.wireguard.com/papers/wireguard-formal-verification.pdf

[39] T. Waldmann, et al., borg – deduplicating archiver (2017).
URL https://borgbackup.readthedocs.io

[40] T. Ylonen, C. Lonvick, RFC 4253: The Secure Shell (SSH) Transport Layer Protocol (2006).
URL https://tools.ietf.org/html/rfc4253

[41] J. Borg, A. Butkevicius, et al., Syncthing specifications (2017).
URL https://docs.syncthing.net/specs/index.html

[42] TOR, Powering Digital Resistance (2018).
URL https://www.torproject.org

[43] T. Hardes, F. Dressler, C. Sommer, Simulating a city-scale community network: From models to first improvements for Freifunk, in: 2017 International Conference on Networked Systems (NetSys), 2017, pp. 1–7. doi:10.1109/NetSys.2017.7903954.

[44] A. G. Bowitz, E. G. Graarud, L. Brown, M. G. Jaatun, BatCave: Adding security to the BATMAN protocol, in: 2011 Sixth International Conference on Digital Information Management, 2011, pp. 199–204. doi:10.1109/ICDIM.2011.6093328.

[45] J. Kelsey and J. Callas and A. Clemm, RFC 5848: Signed Syslog Messages (2010)
URL https://tools.ietf.org/html/rfc5848

[46] NetBSD Project, NetBSD – A fork of the Berkeley Software Distribution (BSD) Operating System.
URL https://www.netbsd.org

[47] Bruce Schneier and John Kelsey, Secure Audit Logs to Support Computer Forensics, ACM Trans. Inf. Syst. Secur. 2 (2) (1999) 159–176. doi:

10.1145/317087.317089.
URL http://doi.acm.org/10.1145/317087.317089

[48] Serguei Popov, The Tangle (2017).
URL https://iota.org/IOTA_Whitepaper.pdf

[49] Dominik Schiener, IOTA introduction at 1st Dutch IOTA Meetup 2017 (2017).

[50] R. Drath and A. Horch, Industrie 4.0: Hit or Hype?, IEEE Industrial Electronics Magazine 8 (2) (2014) 56–58. doi:10.1109/MIE.2014.2312079.

[51] J. Obermaier, M. Hutle, Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems, in: Proceedings of the 2Nd ACM International Workshop on IoT Privacy, Trust, and Security, IoTPTS '16, ACM, New York, NY, USA, 2016, pp. 22–28. doi:10.1145/2899007.2899008.
URL http://doi.acm.org/10.1145/2899007.2899008

[52] S. Notra and M. Siddiqui and H. Habibi Gharakheili and V. Sivaraman and R. Boreli, An Experimental Study of Security and Privacy Risks with Emerging Household Appliances, in: 2014 IEEE Conference on Communications and Network Security, 2014, pp. 79–84. doi:10.1109/CNS.2014.6997469.

[53] H. Hirsch-Kreinsen, Wandel von Produktionsarbeit – Industrie 4.0 (German), Soziologisches Arbeitspapier (38).
URL http://www.wiwi.tu-dortmund.de/wiwi/ts/de/forschung/veroeff/soz_arbeitspapiere/AP-SOZ-38.pdf

[54] Bruce Schneier, The Process of Security (2000).
URL https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

[55] CONFIRM Project, CONFIRM Smart Manufacturing – Transforming Ireland (2018).
URL https://www.confirm.ie

Norbert Wiedermann, M.Sc. is scientific researcher at the Fraunhofer Institute for Applied and Integrated Security (AISEC) since 2013. In his research projects he focuses on IT security aspects for embedded and industrial hardware. By performing risk analysis, developing and implementing security concepts he contributes to increase the protection level for the considered systems.

Sven Plaga received the Dipl. Ing. (FH) and M. Eng. degrees in electrical engineering and computer science from the Deggendorf University of Applied Sciences (Germany) in 2007 and 2010 from the University of Limerick (Ireland), respectively. From 2007 to 2013 he was research fellow at Deggendorf University of Applied Sciences, where he was constantly participated in research projects regarding x86 Embedded Systems. Furthermore, he lectured Embedded Systems and C Programming. Currently, he is a research fellow at Fraunhofer Institute for Applied and Integrated Security (AISEC) and working toward the Ph.D. degree in the field of secure industrial communications in context to embedded systems. Additionally, he assists clients with risk analyses, security concepts and secure implementations within the scope of contracted industrial research projects.

Simon Duque AntÃ³n is a researcher at the German Research Center for Artificial Intelligence (DFKI) working in the â€œIntelligent Networksâ€research group. Born in Hamburg in 1989, he received his Diploma in the field of Computer Science with a specialization in embedded systems in 2015. His main research interests lay in machine learning and its application to the field of industrial IT-security. He is currently working on and coordinating the DFKIâ€™s contribution to the research project IUNO.

Prof. Dr.-Ing- Hans D. Schotten is a full professor and head of the chair for Wireless Communications and Navigation at the University of Kaiserslautern. In addition to that, he is Scientific Director of the Intelligent Networks Research Group of the German Research Center for Artificial Intelligence (DFKI). He received his Ph.D. in Electrical Engineering from the RWTH Aachen in 1997. He was a research group leader there before changing into industry. At Ericsson, he held the position of Senior Researcher, after that he held the position of Director of Technical Standards at Qualcomm. His topics of interest are wireless communication and 5G.

Dr Thomas Newe is a Senior Lecturer in Computer Engineering in the Department of Electronic & Computer Engineering at The University of Limerick and is a funded investigator in the SFI Confirm Manufacturing Centre. He holds a B.Eng. in Computer Engineering, a Masters in Engineering in Security Protocol Design and a PhD in Formal Logics for Security Protocol Verification. He has been a University of Limerick faculty member since 1994. His research interest includes many topics under the general areas of data security for Wireless Sensor Networks and the Internet of Things. He has graduated a number of PhD students in the broad area of network and data security. His students are funded from a variety of sources including: EU, SFI, IRC, Internationally and industrially funded.

Decentralised communication is a important aspect for modern Internet of Things infrastructures.

In industrial use cases decentralised communication gains importance.

Peer to Peer technology provides techniques to establish resilient and secure infrastructures.

Suitable model architectures are developed and presented supporting security by design for industrial Internet of Things environments.

Identified IT security building blocks enable development of sustainable and secure future infrastructures.